Guidelines for the Use of Video Surveillance

October 2015

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

> If all that has to be done to win legal and social approval for surveillance is to point to a social problem and show that surveillance would help to cope with it, then there is no balancing at all, but only a qualifying procedure for a license to invade privacy.
>
> Alan Westin, *Privacy and Freedom*

CONTENTS

FORWARD

The Office of the Information and Privacy Commissioner of Ontario (IPC) first published guidelines for the use of video surveillance in public places in 2001 and then for the use of video surveillance in schools in 2003. The purpose of the guidelines was to assist provincial and municipal public sector institutions (institutions) in determining whether video surveillance programs were lawful and justifiable. These guidelines were subsequently updated in 2007 and 2009, respectively.

Since that time, new circumstances and uses of video surveillance have revealed additional issues and factors to consider. For example, certain circumstances may warrant that you provide individuals with a notice of collection of their personal information in a form other than visual signage. In addition, depending on operational circumstances, the period within which unused video surveillance footage should be erased may vary. Accordingly, we have updated the guidelines to reflect these and other such considerations. We have also restructured the guidelines and provided key messages and examples for clarity.

As noted above, the IPC originally published separate sets of guidelines for the use of video surveillance in public places and in schools. The present guidelines consolidate these documents into a single publication.

INTRODUCTION

Institutions are responsible for ensuring the safety of individuals and the security of equipment and property within the scope of the services they provide. One tool used by institutions to help them fulfill this obligation is video surveillance.

Video surveillance captures sensory information about activities and events in a given area over time. Although primarily used as a means of detecting and assisting in the investigation of criminal activity, video surveillance may also act as a deterrent when used in an appropriate manner.

While video surveillance may help to increase the safety of individuals and the security of assets, it also introduces risks to the privacy of individuals whose personal information may be collected, used and disclosed as a result of the technology. The risk to privacy is particularly acute because video surveillance may, and often does, capture the personal information of law-abiding individuals going about their everyday activities. In view of the broad scope of personal information collected, special care must be taken when considering whether and how to use this technology.

The IPC oversees compliance with the privacy protection provisions of Ontario's *Freedom of Information and Protection of Privacy Act (FIPPA)* and *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, and conducts investigations into privacy complaints. As part of its mandate, the IPC provides guidance, such as that found in this document, regarding Ontario's access and privacy legislation.

The purpose of these guidelines is to inform institutions of their key obligations under *FIPPA* and *MFIPPA* with respect to the use of video surveillance. In addition, they provide a list of best practices which, if implemented, will assist institutions in fulfilling their obligations under *FIPPA* and *MFIPPA* and in protecting the privacy of individuals.

These guidelines are not a comprehensive assessment of every authority or circumstance involving video surveillance in which personal information may be collected, used or disclosed under *FIPPA* and *MFIPPA*. When dealing with issues that may arise in the context of video surveillance, it is important that you consult the acts themselves, including their regulations, and seek advice from your freedom of information and privacy coordinator or legal counsel, where appropriate.

SCOPE OF GUIDELINES

Video surveillance is available in a variety of forms and can be combined with other technologies to augment its capabilities. For example, video surveillance is either covert or overt depending on whether its use is concealed or made known to the individuals affected by it. It is fixed or mobile depending on the range of movement available to it through the technology used. Some examples of mobile video surveillance include body-worn cameras and drones.[1] In addition, video surveillance can be combined with video analytics to increase the identifiability of individuals, patterns of behaviour and objects recorded by it. Some examples of video analytics that may be combined with video surveillance include facial recognition and automated license-plate recognition (ALPR).

While video surveillance is available in different forms and capabilities, these guidelines apply to the use of video surveillance deployed in an *overt* and *fixed* (non-mobile) manner *without* the use of video analytics.

These guidelines do not apply to covert surveillance, or surveillance when used as a case-specific investigation tool for law enforcement purposes where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

These guidelines are also not intended to apply to workplace surveillance systems installed by an institution to conduct surveillance of employees.

VIDEO SURVEILLANCE REQUIREMENTS

In Ontario, *FIPPA* and *MFIPPA* set out rules for the collection, use and disclosure of personal information by institutions. The application of these rules to video surveillance programs raises specific issues. Institutions will need to consider the following issues and the requirements that stem from them when deciding whether and how to use video surveillance.

PERSONAL INFORMATION

The first issue to address when considering the use of video surveillance is whether the system will involve the collection, use or disclosure of personal information. Institutions are required to comply with the rules set out in *FIPPA* and *MFIPPA* with respect to information that falls under the definition of personal information. Section 2(1) of *FIPPA* and *MFIPPA* defines "personal information"

1 For guidance on body-worn cameras, please see the Federal, Provincial and Territorial Privacy Commissioners' "Guidance for the Use of Body-worn Cameras by Law Enforcement Authorities," available on the IPC website.

as “recorded information about an identifiable individual,” which includes, but is not limited to, “information relating to the race, national or ethnic origin, colour, religion, age [or] sex” of the individual.

Therefore, if you use video surveillance to collect, use or disclose personal information, you must comply with the rules set out in *FIPPA* and *MFIPPA*. This will likely be the case, given that video surveillance is typically set up to collect images of individuals from which they may be identified.

EXAMPLE

Use of a video camera in a public school, community college or university that captures identifiable images of students would fall under the purview of *FIPPA* and *MFIPPA*.

LAWFUL COLLECTION

Once you have determined that your video surveillance system will involve the collection of personal information, the next step is to determine whether you have the legal authority to do so. Section 38(2) of *FIPPA* and 28(2) of *MFIPPA* set out the conditions under which personal information may be collected. These sections provide that no person shall collect personal information on behalf of an institution, unless the collection is:

1. expressly authorized by statute,
2. used for the purposes of law enforcement or
3. necessary to the proper administration of a lawfully authorized activity.

At least one of these three conditions must be met in order for you to have the legal authority to collect personal information. You may notice that consent is absent from this list. Unlike under the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which governs most private-sector companies in Canada and federal works and undertakings, consent is not available as a source of authority for the collection of personal information under *FIPPA* or *MFIPPA*. How each of these three conditions for obtaining authority to collect personal information may be met in the case of video surveillance is discussed below.

If you use video surveillance to collect, use or disclose personal information, you must comply with the privacy protections set out in *FIPPA* and *MFIPPA*.

EXPRESSLY AUTHORIZED BY STATUTE

If a statute or regulation provides you with the express authority to collect personal information by means of video surveillance, then you are authorized to do so.

The meaning of this first condition is fairly straightforward. You are authorized to collect personal information if there is a statute or regulation that provides you with such authority and the collection is done in accordance with that statute or regulation and for the specified purpose.

In applying this condition, the qualifier *expressly* must be given additional consideration. The IPC's position is that an authority to collect personal information stated only in broad or non-specific terms would not be enough to be considered "expressly authorized by statute." Instead the phrase:

> requires either that specific types of personal information collected be expressly described in the statute, or a general reference to the activity be set out in the statute, together with a specific reference to the personal information to be collected in a regulation under the statute; i.e., in a form or in the text of the regulation.[2]

Therefore, it is important that you ensure that any statutory authorization to collect personal information by means of video surveillance is grounded in sufficiently specific terms in the applicable statute or regulation.

EXAMPLE

A statutory duty to "take every step reasonable in the circumstances to protect the safety of individuals" would not, on its own, be considered an express authority to collect personal information.

USED FOR THE PURPOSES OF LAW ENFORCEMENT

The wording of this second condition can give rise to some confusion. Does it mean that *any* institution can be authorized to collect personal information so long as it is "used for the purposes of law enforcement?" Or, is it restricted in its application to those institutions with a law enforcement mandate?

The IPC's position is the latter: the institution must have a clear law enforcement mandate, ideally in the form of a statutory duty. As per the definition of "law enforcement" in section 2(1) of *FIPPA* and *MFIPPA*, this could be either with respect

2 See Investigation Report I95-030P, available on the IPC website.

to "policing" or "investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings." Therefore, to justify the collection of personal information under this condition, it is not enough to claim a mere *interest* in policing or law enforcement investigations.[3]

If your institution has a clear law enforcement mandate, then you are authorized to collect personal information by means of video surveillance, so long as that collection furthers actual law enforcement purposes.

At the same time, those institutions that do in fact have a clear law enforcement mandate—for example, police services, certain kinds of regulators, transit authorities with special constable services[4]—are not granted *carte blanche* under this law enforcement condition. In Privacy Complaint Report MC-040012-1, the IPC held that the phrase "used for the purposes of law enforcement" is not an unconditional authority and only applies in cases where the collection of personal information furthers actual law enforcement purposes.[5] Accordingly, the considerations set out in the next section, especially in regard to the "necessity" of the collection of personal information, will, in general, also apply to the use of video surveillance by law enforcement agencies.

NECESSARY TO THE PROPER ADMINISTRATION OF A LAWFULLY AUTHORIZED ACTIVITY

This condition may authorize a collection of personal information in a wide range of circumstances. To satisfy this condition, you must be able to demonstrate two things: (1) that the activity for which personal information is collected is "lawfully authorized," and (2) that the collection of personal information is "necessary" to that activity.

LAWFULLY AUTHORIZED

In understanding what is meant by "lawfully authorized activity," it is important to note that the activity at issue, while related to the activity of collecting personal information, is not identical to it. The lawfully authorized activity forms the context within which the collection would occur. In the case of video surveillance, the activity will typically relate to the safe and secure operation of a building, facility or public space.

With respect to the phrase "lawfully authorized," the authorization may come in different forms—for example, in a statute or regulation, but also in a bylaw, policy or

3 See Investigation Report I95-030P available on the IPC website.
4 See Privacy Investigation Report MC07-68 "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report" available on the IPC website.
5 Privacy Complaint Report MC-040012-1 available on the IPC website.

order formally approved by a governing body with the lawful authority to enact such a bylaw, policy or order.

EXAMPLE

A school board is lawfully authorized to operate a school under the *Education Act* and, in doing so, it must take reasonable steps to ensure the safety and security of students and property. Similarly, municipalities are lawfully authorized to operate municipal community centres and, in doing so, they are required to take steps to ensure the safety of the individuals who visit such centres.

NECESSARY

In addition to being part of a lawfully authorized activity, the third condition for legal authority to collect personal information under section 38(2) of *FIPPA* and section 28(2) of *MFIPPA* requires that the collection of personal information be "necessary" to the proper administration of that activity. "Necessary" here means *more* than merely helpful. Accordingly, a collection of personal information that was only merely helpful to the proper administration of a lawfully authorized activity would not meet the "necessary" standard.[6]

In determining whether the collection of personal information is "necessary," it is important to consider the necessity of the collection from the following aspects:

1. the means used to collect the personal information,
2. the sensitivity of the personal information and
3. the amount of personal information.

The authority for the lawfully authorized activity may come in the form of a statute or regulation, but also in a bylaw, policy or order formally approved by a governing body with the lawful authority to do so.

The Means Used to Collect Personal Information

As noted in the Introduction, a particularly privacy-invasive aspect of video surveillance is that it frequently collects the personal information of law-abiding individuals going about their everyday activities. Because of this, when determining the necessity of video surveillance as a means to collect personal information, it is important that you consider whether the following circumstances hold:

6 See *Cash Converters Canada Inc v Oshawa (City),* 2007 ONCA 502 at para 40.

- The problem to be addressed by video surveillance is real, substantial and pressing. Note that this may be shown on the basis of verifiable, specific incidents of crime or significant safety concerns.

EXAMPLE

A minor offence such as littering would, in general, not be considered a substantial or pressing problem. It would, therefore, not meet the required criteria to justify the use of video surveillance.

- Other less intrusive means of achieving the same goals have been considered and are substantially less effective than video surveillance or are not feasible.

EXAMPLE

A dimly lit area of a public school has been the site of ongoing vandalism and violence. Before considering video surveillance, the school should evaluate the effectiveness of less intrusive alternatives such as increased lighting and foot patrols.

- The benefits of video surveillance substantially outweigh the reduction of privacy inherent in its use. Note that an overall reduction in costs will not, in and of itself, be considered sufficient to outweigh the reduction in privacy.

The feeling of being watched or monitored by the continuous "gaze" of video surveillance may have a "chilling effect" on law-abiding individuals, causing them to alter their behaviour and limit the expression of their rights. When weighing the benefits of video surveillance against the costs to privacy, institutions should keep these kinds of potential effects of video surveillance in mind.

The Sensitivity of Personal Information

In the case of video surveillance, the sensitivity of the personal information collected will inform whether the benefits of video surveillance, discussed above, will substantially outweigh the reduction of privacy inherent in its use. The loss of privacy is directly related to the sensitivity of the personal information involved. Therefore, the greater the sensitivity of the personal information collected, the greater the benefits of video surveillance must be in order to substantially outweigh the reduction in privacy.

When determining the sensitivity of personal information collected by means of video surveillance, it is important that you consider the following two factors: (1) the nature of the space under observation, and (2) the "closeness" of the surveillance.

Determining the sensitivity of personal information collected by means of video surveillance requires consideration of the nature of the space under observation and the "closeness" of the surveillance.

Some spaces are considered to be more sensitive than others. For example, individuals generally have a higher expectation of privacy in areas such as change rooms and public washrooms. Accordingly, the sensitivity of these semi-private spaces would be considered to be higher than that of "open air" public spaces such as public roads, parks and squares, where individuals generally have a lower expectation of privacy. Although generally lower, individuals' expectation of privacy in public space is not entirely eliminated.[7]

At the same time, a space in which individuals generally have a lower expectation of privacy can be made more sensitive as a result of the means used to collect personal information. For example, if the video surveillance technology in use can zoom in on individuals sitting in a public park such that it is able to read the words they are reading or writing, then the sensitivity of that space and the personal information collected in it would increase. In addition, the sensitivity of the information may rise when the recording is continuous, particularly where the information is not subject to a short retention period.

The Amount of Personal Information

This factor involves applying the principle of data minimization to the collection and storage of personal information. In the case of video surveillance, data minimization entails limiting the amount of personal information collected and retained to that which is necessary to fulfill the purposes of the lawfully authorized activity. With respect to limiting the amount of personal information collected, it is important that you consider making the following adjustments when installing and operating the surveillance equipment:

- Recording equipment, such as video cameras, audio recorders or other devices, is installed only in areas directly related to the problem to be addressed by video surveillance.
- Additional sensory information, such as sound, is not recorded or made available to operators unless it is directly related to the problem to be addressed by video surveillance.

7 See *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 27; and see Privacy Investigation Report MC07-68 "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report" at page 2, available on the IPC website.

- Reception equipment is installed and set up such that it monitors only those spaces that have been identified as requiring video surveillance. For example, cameras should not be directed to look through the windows of adjacent buildings or onto adjacent property, or else those areas should be blocked from view or blacked out.
- If the capabilities of the reception equipment are adjustable by operators, these capabilities have been restricted, to the extent possible, so that operators cannot adjust, zoom or otherwise manipulate the equipment to collect information about spaces that are not intended to be covered by the video surveillance program.

Ensure that the amount of personal information collected by means of video surveillance is limited to that which is necessary by adjusting the number of cameras and the installation and operation of the surveillance equipment accordingly.

In addition, you may wish to consider restricting video surveillance to time periods when there is a demonstrably higher likelihood of the presence of the underlying problem in the area under surveillance.

EXAMPLE

A video camera that monitors a parking lot indirectly captures information about adjacent properties. To limit the amount of personal information collected by it, the camera is set up to automatically avoid or black out any area or property adjacent to the parking lot.[8]

With respect to limiting the amount of personal information retained, because video surveillance frequently collects the personal information of law-abiding individuals going about their everyday activities, a large portion of the footage collected will not be used. In order to protect this unused footage from misuse, it is important that you limit its retention period in the following way:

- Recorded information that has not been used is routinely erased according to a standard schedule. Under the standard schedule, the retention period for unused information is limited to the amount of time reasonably necessary to discover or report an incident that occurred in the space under surveillance.

8 For additional information involving a similar case, see Privacy Complaint Report MC13-60, available on the IPC website.

When erasing or deleting recorded information, whether used or unused, it is critical that the information and old storage devices are disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.[9]

EXAMPLE

In Privacy Complaint MC13-46, the IPC reviewed the video surveillance practices of a public school which included routinely erasing unused personal information collected by its video surveillance system according to a standard schedule of 20 days, at most. Because the school is not operational year round and is often closed for extended periods over the holidays and summer, the IPC upheld this retention period, as there may be a delay between when an incident occurs and its discovery.[10]

NOTICE OF COLLECTION

FIPPA and *MFIPPA* require that individuals be notified of the collection of their personal information, subject to specific and narrow exceptions.[11] Specifically, section 39(2) of *FIPPA* and section 29(2) of *MFIPPA* provide that an individual must be informed of:

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Ensure that the retention period for unused information is limited to the amount of time reasonably necessary to discover or report an incident that occurred in the space under surveillance.

Providing effective notice in the context of video surveillance may be challenging because the collection occurs automatically—simply by virtue of individuals moving or finding themselves within a particular space monitored by video surveillance. Accordingly, it is important that you consider implementing the following conditions:

9 For guidance on the secure destruction of personal information, see "Secure Destruction of Personal Information," available on the IPC website.

10 See Privacy Complaint MC13-46, available on the IPC website.

11 See section 39(3) of *FIPPA* and section 29(3) of *MFIPPA*.

- Signs with a clear, language-neutral graphical depiction of the use of video surveillance are prominently displayed at the perimeter of the monitored areas and at key locations within the areas. The signs should include basic information to clarify that video surveillance is being used in the area.
- The information required by paragraphs (a)–(c) of section 39(2) of *FIPPA* and section 29(2) of *MFIPPA* is available and easily accessible on your institution's website.

The above guidance for signs assumes that a high percentage of the individuals whose personal information is being collected are able to read them—in other words, that they are not visually disabled. However, this may not be the case in certain spaces, such as services dedicated to persons with physical disabilities. In such cases, it is important that you consider providing notice in alternative forms

EXAMPLE

A public transportation service for individuals with physical disabilities should provide an alternative notice of collection to blind or visually impaired customers.

LAWFUL USE

Because video surveillance collects a broad scope of personal information, much of the information collected is not likely to be relevant to the purpose of the surveillance program. For example, a security camera set up to monitor the entrance to a school will typically collect more information about the movements and activities of law-abiding individuals going about their everyday activities than information relating to security incidents. An important aspect of managing a video surveillance program involves protecting this additional personal information from misuse.

Section 41(1) of *FIPPA* and section 31(1) of *MFIPPA* restrict how personal information may be used once it has been lawfully collected. As a general rule, the acts prohibit the use of personal information unless the institution obtains consent from the individual to whom

Ensure that notice of collection is provided to individuals on the institution's website and the use of signs with the required information and a clear, language-neutral, graphical depiction of the use of video surveillance is prominently displayed at the perimeter of the monitored areas and at key locations within these areas. It may also be necessary for you to provide notice in alternative forms for persons with visual disabilities.

the information relates or the personal information is used for the purpose for which it was obtained or compiled or for a consistent purpose. A "consistent purpose" is defined in section 43 of *FIPPA* and section 33 of *MFIPPA* as a use of personal information that the individual to whom the information relates might reasonably have expected at the time of collection.

In the context of video surveillance, this means that as a general rule, institutions may only use personal information collected by means of video surveillance for the purpose of the video surveillance program or for a consistent purpose. Use of the information for other, unrelated purposes would not generally be permitted. When information collected for one purpose is used for another, unrelated purpose this is often called "function creep."

EXAMPLE

In the school context referred to above, the personal information collected by the security camera may not be used to monitor student attendance or evaluate school uniform infractions, but it may be used in relation to a security incident.

LAWFUL DISCLOSURE

FIPPA and *MFIPPA* prohibit the disclosure of personal information, except in the circumstances identified in section 42(1) of *FIPPA* and 32 of *MFIPPA*. You should develop policies and procedures in consultation with your freedom of information and privacy coordinator or legal counsel to ensure that any disclosures of video surveillance footage are consistent with these sections.

While personal information may be lawfully disclosed in these limited circumstances, an increasingly important issue in the context of video surveillance is the disclosure of personal information to appropriate authorities, above all, law enforcement agencies.

The existence of video surveillance in spaces managed by institutions has not gone unnoticed by law enforcement agencies, who increasingly rely upon it as an additional evidentiary tool in investigations, including into incidents that did not directly occur in those spaces. If your institution uses video surveillance, you may receive requests from law enforcement agencies for footage relating to incidents of which you have no

As a general rule, an institution is prohibited from using personal information collected by means of video surveillance, unless it is used for the purpose of the video surveillance program or for a consistent purpose.

prior knowledge. At other times, you may consider disclosing footage to a law enforcement agency on your own initiative, for example, in response to illegal activity that occurs on the premises of your institution.

While there may be other situations where the disclosure of video surveillance footage is permitted, video surveillance may be disclosed to a law enforcement agency when:

- the law enforcement agency approaches your institution with a warrant requiring the disclosure of the footage, as per section 42(1)(e) of *FIPPA* and section 32(e) of *MFIPPA*,
- the law enforcement agency approaches your institution, without a warrant, and asks that you disclose the footage to aid an investigation from which a proceeding is likely to result, as per section 42(1)(g) of *FIPPA* and section 32(g) of *MFIPPA* or
- you observe an illegal activity on your premises and disclose the footage to a law enforcement agency to aid an investigation from which a proceeding is likely to result, as per section 42(1)(g) of *FIPPA* and section 32(g) of *MFIPPA*.

EXAMPLE

An institution learns of an alleged assault in an area monitored by video surveillance. Upon reviewing the relevant footage, the institution may report the incident and disclose the footage to the police.

When permitted under *FIPPA* or *MFIPPA*, it is important that disclosures be done in a manner that protects the privacy and security of the personal information. Section 4 of Regulation 460 of *FIPPA* and section 3 of Regulation 823 of *MFIPPA* require institutions to define, document and put in place reasonable measures to prevent unauthorized access as well as inadvertent destruction or damage of records. Accordingly, when disclosing personal information, it is important that you:

- Maintain an auditable log of each disclosure.
- Ensure the log includes the date, time and location of the footage and, where applicable, the case file number of the law enforcement agency's investigation.

- Ensure the log also includes a description of the circumstances justifying the disclosure, the amount of footage involved, the name, title and agency to whom the footage is being disclosed, the legal authority for the disclosure, the means used to disclose the footage and whether the footage will be returned or securely destroyed after use.
- Ensure that if digitized, the footage is securely encrypted.

Ensure that reasonable measures to prevent unauthorized access and inadvertent destruction or damage of records are defined, documented and put in place as part of your institution's process for disclosing video surveillance footage.

ACCESS

Individuals have a general right of access to records in the custody or under the control of institutions, under section 10 of *FIPPA* and section 4 of *MFIPPA*. Additionally, individuals whose personal information is in the custody or under the control of institutions have a right of access to that personal information under section 47(1) of *FIPPA* and section 36(1) of *MFIPPA*.

Ensure that your video surveillance program includes a process for responding to access to information requests and the means to redact exempt information from the video footage.

Your institution may receive a request from an individual for access to surveillance footage capturing his or her image for specified periods of time. That individual may have a right to access the relevant footage. Accordingly, you should ensure that your institution has a process in place to facilitate responses to access to information requests. Note that all or portions of the video surveillance footage requested may be exempt from disclosure for a number of reasons under *FIPPA* and *MFIPPA*, including the fact that disclosure may result in an unjustified invasion of someone else's privacy.[12]

In addition, your video surveillance system should include the ability to remove or redact information from the video footage to protect exempted information—for example, by using tools and techniques such as:

- digitizing analogue footage to enable the use of more powerful editing tools,
- blacking out or blurring images of individuals and
- removing the sound of voices.

12 The video surveillance footage may also be exempt from disclosure for other reasons. You will need to consult with your freedom of information and privacy coordinator or legal counsel regarding the request and the information that should be redacted.

EXAMPLE

An individual slips and falls on a staircase in a subway station in front of several bystanders, and the accident is recorded by the transit authority's video surveillance system. If the individual makes an access request for information relating to that incident, fulfilling the request may involve a record that contains the personal information of the bystanders as well as the individual. To protect the privacy of the bystanders, it may be necessary to obscure their personal information before the record is disclosed to the requester.

RETENTION

To ensure that individuals have a reasonable opportunity to access the personal information about them held by institutions, *FIPPA*, *MFIPPA* and their regulations set out rules regarding the minimum length of time institutions must retain personal information once they have used it. Specifically, section 5(1) of Regulation 460 of *FIPPA* and section 5 of Regulation 823 of *MFIPPA* require institutions in general to retain personal information for at least one year after use, although Regulation 823 permits municipal institutions to reduce this time period through a resolution or bylaw.

It is important to note that this retention requirement applies only to personal information that has been "used" by institutions. It does not apply to personal information that has been collected but not used, which in the case of video surveillance may have much shorter retention requirements.[13] In the context of video surveillance, personal information is used whenever footage that contains images of individuals or other identifiable information is accessed or disclosed. Therefore, if you access or disclose video surveillance footage, as a general rule it is important that you retain it for at least one year.[14] However, simply viewing a live feed does not represent a "use" of personal information.

If your institution accesses or discloses video surveillance footage, as a general rule, retain the footage for at least one year to provide the individuals to whom it relates with an opportunity to access it.

SECURITY

Section 4 of Regulation 460 of *FIPPA* and section 3 of Regulation 823 of *MFIPPA* require institutions to protect personal information in their custody or under their control from unauthorized access and inadvertent destruction or damage.

13 See the retention requirement in the discussion of "The Amount of Personal Information" above.

14 Note that your institution may have records retention requirements and policies that require the retention of used, accessed or disclosed video surveillance footage beyond the one year retention period set out in *FIPPA* and *MFIPPA*.

In the context of video surveillance, security involves ensuring the confidentiality, integrity and availability of the footage captured by the system. Accordingly, it is important that you define, document and put in place reasonable measures to safeguard the video surveillance footage in your custody or under your control. These measures may include:

- strongly encrypting video surveillance footage at rest and when transmitted across open, public networks,
- storing physical records of footage, such as discs, memory cards or servers, in a locked facility,
- limiting staff and other individuals' access to footage on a need-to-know basis,
- storing monitors in a secure location where they are not visible to the public,
- granting accounts, systems, applications and devices only the degree and kind of access necessary to fulfill defined duties and functions,
- whitelisting applications to help prevent malware and other non-approved programs from running,
- regularly patching systems and applications to protect against vulnerabilities,
- using standard, secure system configurations and not using default or factory settings and
- keeping auditable logs of all accesses, uses and disclosures of footage that are generated automatically where records are maintained electronically.

Define, document and put in place reasonable measures to safeguard the video surveillance footage in the custody or under the control of your institution.

You may need to consult with the system provider and/or technical staff to implement some of these measures.

If you are considering storing video surveillance footage outside of Canada—for example, if you use a third-party service provider with data centres located outside of Canada—you should perform a risk-based analysis to determine whether the risks posed by the extraterritorial storage of personal information can be sufficiently mitigated by applicable safeguards, such as contractual provisions. This analysis will take into consideration the sensitivity of the footage and the laws of the jurisdiction in which the personal information is to be stored.[15]

15 For additional guidance on U.S.-based service providers, please see Privacy Investigation Report PC12-39 "Reviewing the Licensing Automation System of the Ministry of Natural Resources", available on the IPC website.

VIDEO SURVEILLANCE BEST PRACTICES

Knowing your institution's obligations under *FIPPA* and *MFIPPA* is one thing; fulfilling them, however, is another. While the above section seeks to inform institutions of their obligations under *FIPPA* and *MFIPPA* with respect to the use of video surveillance, it does not discuss organizational procedures that institutions may implement towards achieving and maintaining compliance. In what follows, we will discuss five best practices to assist institutions in fulfilling their obligations under *FIPPA* and *MFIPPA* and in protecting the privacy of individuals.

PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is a risk management tool that helps to identify the effects of a given program or other activity on an individual's privacy, and the safeguards or strategies that may be employed to eliminate the adverse outcomes of those effects or reduce them to an acceptable level. These safeguards and strategies can then be incorporated into the institution's video surveillance program, policies and procedures. PIAs also serve to identify risks to organizations.

Conduct a PIA to identify and address the issues raised by your institution's use of video surveillance.

Many of the issues raised in the previous section of these guidelines will be addressed in the course of conducting a PIA, if done properly. A PIA should, for example, identify and help resolve issues relating to your institution's use of video surveillance, including:

- the lawfulness of the collection, use, disclosure and retention of personal information,
- requirements for notice and individual access and
- appropriate measures to safeguard personal information.

Therefore, it is important that you conduct a PIA prior to your institution's use of video surveillance and whenever significant changes are made to the program. Institutions may wish to refer to the IPC's *Planning for Success: Privacy Impact Assessment Guide*[16] or to the Ministry of Government and Consumer Services' PIA guidelines and tools[17] for guidance on completing a PIA, or other guidance that may be directly applicable to your institution.

16 Available on the IPC website.

17 Available by contacting the Information, Privacy and Archives Division by email at web.foi.MGCS@ontario.ca or by telephone at 416-212-7061.

PUBLIC CONSULTATION

Demonstrating that you have considered all the issues raised by the use of video surveillance and have made informed decisions regarding them promotes accountability on the part of your institution and increases public trust in the program. The use of video surveillance affects all the individuals who end up moving within the space under observation. Therefore, prior to using video surveillance, and where feasible to do so, you should identify those who reasonably may be affected by the video surveillance and consult with them as to the program's necessity and impact. This consultation provides stakeholders with an opportunity to comment on the specifics of the program—for example, the location of cameras—in addition to the use of video surveillance itself. You should also develop a process for evaluating the necessity of the program on an ongoing basis and stakeholder consultations should be part of that process. Additionally, it is important that you consider consulting with stakeholders prior to updating your institution's surveillance equipment or practices.

Consult with the public as to the necessity and impact of the proposed use of video surveillance.

POLICIES AND PROCEDURES

Institutions should develop and implement policies and procedures to assist in complying with the requirements set out in section 4 of Regulation 460 of *FIPPA* and section 3 of Regulation 823 of *MFIPPA*. These provisions require institutions to define, document and put in place reasonable measures to safeguard the video surveillance footage in your custody or under your control.[18] While security is necessary, implementing policies and procedures for all aspects of your video surveillance program will help you to fulfill your obligations under *FIPPA* and *MFIPPA*. Accordingly, it is important that comprehensive policies and procedures for your institution's use of video surveillance be developed and implemented. These policies and procedures may include information about the issues raised above in these guidelines, such as:

- A description of the status of your institution under *FIPPA* or *MFIPPA* and the duties and responsibilities that arise as a result of this status. This may include your institution's obligations with respect to notice, access, use, disclosure, retention and disposal of records in accordance with *FIPPA* and *MFIPPA*.
- The rationale, objectives and justification for implementing the video surveillance program.

18 See the 'Security' section of these guidelines.

- A description of the nature of the personal information collected.
- Limitations placed on access to and use of personal information by employees, including the individuals that can view the information and under what circumstances it may be viewed.
- A description of the procedure that must be followed in the event that an employee is requested to disclose personal information.
- The potential consequences to employees if they breach policies or procedures.
- The designation of a senior staff member to be responsible for the organization's privacy obligations under *FIPPA* or *MFIPPA* and its policy.
- The administrative, technical and physical safeguards implemented by the organization to prevent unauthorized access to personal information and to protect personal information from inadvertent destruction or damage.
- The duties and responsibilities of employees in implementing the administrative, technical and physical safeguards put in place. This includes the signing of a written agreement to adhere to these duties, including an undertaking of confidentiality, and to undergo initial and ongoing privacy training.
- An explanation of the process for responding to privacy breaches and the duties and responsibilities imposed on employees in identifying, reporting, containing and participating in the investigation and remediation of privacy breaches.[19]
- The retention periods of the surveillance footage.
- The frequency and circumstances in which the video surveillance program will be audited.

In addition, it is important that you consider reviewing and updating your institution's policies and procedures regularly or whenever there is a change or upgrade to the video surveillance program. You may also consider making these policies and procedures available to the public.

Develop and implement comprehensive policies and procedures for your institution's use of video surveillance, and update the policies and procedures when changes are made to the program, for example, when equipment is upgraded.

19 See *Privacy Breach Protocol & Guidelines for Government Organizations*, available on the IPC website.

TRAINING

Train employees to ensure that they understand their duties and responsibilities under *FIPPA* and *MFIPPA* with respect to your institution's video surveillance program.

Educating your employees on their roles and responsibilities, as defined in the policies and procedures you have developed, is an essential step to achieving an effective and compliant video surveillance program. How are employees to know what their individual duties and responsibilities are if they are not adequately trained on them? If employees are not aware of their roles and responsibilities, your institution may be at a greater risk of having a privacy breach. Accordingly, it is important that employees be trained to ensure that they understand their duties and responsibilities under *FIPPA* and *MFIPPA* with respect to your institution's video surveillance program. Specifically, it is recommended that employees attend an initial privacy orientation as well as regular training, and that these training programs contain detailed information about the policies and procedures that have been implemented by the organization and the obligations arising from them.

AUDITS

While developing policies and procedures and training employees are important steps to achieving an effective and compliant project or program, doing this does not necessarily mean that the roles, responsibilities and practices set out in the policies and procedures are, in fact, being followed or have been realized within an institution. To achieve this next level of assurance, verification of your institution's compliance with its policies and procedures is needed. Accordingly, it is important that you audit the roles, responsibilities and practices of your institution's video surveillance program regularly to ensure that they comply with your policies and procedures[20]. You may wish to consider retaining an independent third party to perform the audit.

In addition, the circumstances under which the use of video surveillance was originally justified may change. An area that was once prone to high rates of criminal activity may, through development or other external factors, transform into a low-crime area. Further, new, less intrusive means of achieving the same goals may become available. Accordingly, it is important that the necessity of your institution's video surveillance program regularly be considered to determine whether it is still justified in accordance with the requirements under *FIPPA* and *MFIPPA*.

20 There may be circumstances where it would be appropriate to conduct audits more frequently, including where a previous inappropriate access or disclosure or other privacy breach has occurred.

When performing an audit, it is important that you address any deficiencies or concerns identified by the audit in a timely fashion, in some cases immediately. It is also important that you inform employees of the fact that their job activities may be subject to auditing and that they may be called upon to justify particular instances where they accessed footage. Further, in the interest of openness and transparency, you may wish to make the findings of your audit publicly available.

Audit the roles, responsibilities and practices of your institution's video surveillance program regularly to ensure that they comply with your policies and procedures. Review and evaluate the necessity of your institution's video surveillance program regularly to determine whether it is still justified in accordance with the requirements under *FIPPA* and *MFIPPA*.

CONCLUSION

Institutions are increasingly looking to video surveillance to assist in maintaining the safety of individuals and the security of property within their institutions. By its very nature, video surveillance introduces risks to the privacy of individuals whose personal information may be collected, used and disclosed. However, if the program associated with the use of video surveillance is implemented in a privacy-protective manner, as described in these guidelines, the risks may be sufficiently mitigated to fulfill institutions' obligations under *FIPPA* and *MFIPPA*. These guidelines present various issues, requirements and best practices for institutions to consider before as well as after implementing a video surveillance program.

ADDITIONAL RESOURCES

IPC Privacy Complaint Reports involving video surveillance on the IPC website:

- Privacy Complaint MC13-60
- Privacy Complaint MC13-46
- Privacy Complaint MC10-2
- Privacy Investigation Report MC07-68, Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three *Acts*, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction.**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations.**
- **Conducts research into access and privacy issues.**
- **Comments on proposed government legislation and programs.**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Website: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

October 2015